

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application:

2002年 9月26日

出 願 番 号

Application Number:

特願2002-280289

[ST.10/C]:

[JP2002-280289]

出 願 人

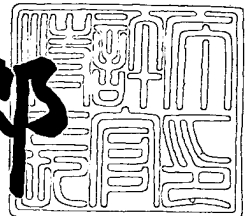
Applicant(s):

株式会社東芝

2003年 3月 7日

特 許 庁 長 官
Commissioner,
Japan Patent Office

太田 信一郎



出証番号 出証特2003-3014090

【書類名】 特許願

【整理番号】 13B0250501

【あて先】 特許庁長官殿

【国際特許分類】 H04L 12/00

【発明の名称】 サーバ計算機保護装置、サーバ計算機保護方法、サーバ計算機保護プログラム及びサーバ計算機

【請求項の数】 10

【発明者】

【住所又は居所】 神奈川県川崎市幸区小向東芝町 1 番地 株式会社東芝
研究開発センター内

【氏名】 菅野 伸一

【発明者】

【住所又は居所】 東京都府中市東芝町 1 番地 株式会社東芝 府中事業所
内

【氏名】 楯岡 正道

【特許出願人】

【識別番号】 000003078

【氏名又は名称】 株式会社 東芝

【代理人】

【識別番号】 100083161

【弁理士】

【氏名又は名称】 外川 英明

【電話番号】 (03)3457-2512

【手数料の表示】

【予納台帳番号】 010261

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】	要約書	1
【プルーフの要否】	要	

【書類名】 明細書

【発明の名称】 サーバ計算機保護装置、サーバ計算機保護方法、サーバ計算機保護プログラム及びサーバ計算機

【特許請求の範囲】

【請求項 1】

不特定のクライアント計算機によるDoS攻撃からサーバ計算機を保護するサーバ計算機保護装置において、

クライアント計算機から送られてくるデータ要求をサーバ計算機の代わりに受け付けるデータ要求受け付け手段と、

一定期間内に、すべてのクライアント計算機から届いたデータ要求の数を計測するデータ要求数計測手段と、

一定期間内に前記サーバ計算機から前記クライアント計算機へ応答した数を計測するデータ応答数計測手段と、

前記データ応答数計測手段及びデータ要求数計測手段の出力結果を用いて前記サーバ計算機の負荷状態を求めるサーバ負荷算出手段と、

前記サーバ負荷算出手段によって求めた負荷状態に応じて、一定期間内に前記データ要求受け付け手段が受け付けたデータ要求のうちの、該受け付けたデータ要求数に対する一定期間内に前記サーバ計算機へ転送するデータ要求の数の割合を変化させるデータ要求転送手段と、

を備えたことを特徴とするサーバ計算機保護装置。

【請求項 2】

不特定のクライアント計算機によるDoS攻撃からサーバ計算機を保護するサーバ計算機保護装置において、

所定のクライアント計算機から送られてくるデータ要求をサーバ計算機の代わりに受け付けるデータ要求受け付け手段と、

一定期間内に、前記所定のクライアント計算機から届いたデータ要求の数を計測するデータ要求数計測手段と、

一定期間内に前記サーバ計算機が前記所定のクライアント計算機へ応答した数を計測するデータ応答数計測手段と、

前記データ要求数計測手段及びデータ応答数計測手段の出力結果を用いて、前記所定のクライアント計算機に対するサーバ計算機の負荷状態を求めるサーバ負荷算出手段と、

前記サーバ負荷算出手段によって求めた負荷状態に応じて、一定期間内に前記データ受け付け手段が受け付けた前記所定のクライアント計算機から送られてくるデータ要求のうちの、該受け付けたデータ要求数に対する一定期間内に前記サーバ計算機へ転送するデータ要求の数の割合を変化させるデータ要求転送手段と

を備えたことを特徴とするサーバ計算機保護装置。

【請求項 3】

前記データ要求転送手段は、前記サーバ負荷算出手段が求めた前記サーバ計算機の負荷状態から、以前よりも負荷が高くなったと判断した場合は前記サーバ計算機へ転送するデータ要求の数の割合をより低く設定し、

一方、以前よりも負荷が低くなったと判断した場合は前記サーバ計算機へ転送するデータ要求の数の割合をより高く設定することを特徴とする請求項 1 または請求項 2 に記載のサーバ計算機保護装置。

【請求項 4】

不特定のクライアント計算機による DoS 攻撃からサーバ計算機を保護するサーバ計算機保護方法であって、

クライアント計算機から送られてくるデータ要求をサーバ計算機の代わりに受け付けるステップと、

一定期間内に、すべてのクライアント計算機から届いたデータ要求の数を計測するステップと、

一定期間内に前記サーバ計算機から前記クライアント計算機へ応答した数を計測するステップと、

前記データ要求数及び応答数を用いて前記サーバ計算機の負荷状態を求めるステップと、

前記求めた負荷状態に応じて、一定期間内に受け付けた前記データ要求のうちの、該受け付けたデータ要求数に対する一定期間内に前記サーバ計算機へ転送す

るデータ要求の数の割合を変化させるデータ要求転送ステップと、
を有することを特徴とするサーバ計算機保護方法。

【請求項 5】

不特定のクライアント計算機によるDoS攻撃からサーバ計算機を保護するサーバ計算機保護方法であって、

所定のクライアント計算機から送られてくるデータ要求をサーバ計算機の代わりに受け付けるステップと、

一定期間内に、前記所定のクライアント計算機から届いたデータ要求の数を計測するステップと、

一定期間内に前記サーバ計算機が前記所定のクライアント計算機へ応答した数を計測するステップと、

前記データ要求数及び応答数を用いて、前記所定のクライアント計算機に対するサーバ計算機の負荷状態を求めるステップと、

前記求めた負荷状態に応じて、一定期間内に受け付けた前記所定のクライアント計算機から送られてくるデータ要求のうちの、該受け付けたデータ要求数に対する一定期間内に前記サーバ計算機へ転送するデータ要求の数の割合を変化させるデータ要求転送ステップと、

を有することを特徴とするサーバ計算機保護方法。

【請求項 6】

前記データ要求転送ステップは、求めた前記サーバ計算機の負荷状態から、以前よりも負荷が高くなったと判断した場合は前記サーバ計算機へ転送するデータ要求の数の割合をより低く設定し、

一方、以前よりも負荷が低くなったと判断した場合は前記サーバ計算機へ転送するデータ要求の数の割合をより高く設定することを特徴とする請求項 4 または請求項 5 に記載のサーバ計算機保護方法。

【請求項 7】

不特定のクライアント計算機によるDoS攻撃からサーバ計算機を保護するサーバ計算機保護プログラムであって、

所定のクライアント計算機から送られてくるデータ要求をサーバ計算機の代わ

りに受け付けるステップと、

一定期間内に、前記所定のクライアント計算機から届いたデータ要求の数を計測するステップと、

一定期間内に前記サーバ計算機が前記所定のクライアント計算機へ応答した数を計測するステップと、

前記データ要求数及び応答数を用いて、前記所定のクライアント計算機に対するサーバ計算機の負荷状態を求めるステップと、

前記求めた負荷状態に応じて、一定期間内に受け付けた前記所定のクライアント計算機から送られてくるデータ要求のうちの、該受け付けたデータ要求数に対する一定期間内に前記サーバ計算機へ転送するデータ要求の数の割合を変化させるデータ要求転送ステップと、
を有することを特徴とするサーバ計算機保護プログラム。

【請求項 8】

前記データ要求転送ステップは、求めた前記サーバ計算機の負荷状態から、以前よりも負荷が高くなったと判断した場合は前記サーバ計算機へ転送するデータ要求の数の割合をより低く設定し、

一方、以前よりも負荷が低くなったと判断した場合は前記サーバ計算機へ転送するデータ要求の数の割合をより高く設定することを特徴とする請求項 7 に記載のサーバ計算機保護プログラム。

【請求項 9】

クライアント計算機からの要求に応じたデータを供給するサーバ計算機であって、

所定のデータ要求を処理して、該データ要求をしたクライアント計算機に供給するデータを作成するデータ処理手段と、

所定のクライアント計算機から送られてくるデータ要求を受け付けるデータ要求受け付け手段と、

一定期間内に、前記所定のクライアント計算機から届いたデータ要求の数を計測するデータ要求数計測手段と、

一定期間内に、前記所定のクライアント計算機へ応答した数を計測するデータ

応答数計測手段と、

前記データ要求数計測手段及びデータ応答数計測手段の出力結果を用いて、前記所定のクライアント計算機に対する負荷状態を求めるサーバ負荷算出手段と、

前記サーバ負荷算出手段によって求めた負荷状態に応じて、一定期間に前記データ受け付け手段が受け付けた前記所定のクライアント計算機から送られてくるデータ要求のうちの、該受け付けたデータ要求数に対する一定期間内に前記データ処理手段へ転送するデータ要求の数の割合を変化させるデータ要求転送手段とを備え、

不特定のクライアント計算機からのDoS攻撃を受けたときに、正当なデータ要求を行っていた所定のクライアント計算機からのデータ要求、および正当なデータ要求を行っているにもかかわらず、DoS攻撃を行っていると判断された所定のクライアント計算機からのデータ要求が継続して処理されること特徴とするサーバ計算機。

【請求項 10】

前記データ要求転送手段は、前記サーバ負荷算出手段が求めた前記サーバ計算機の負荷状態から、以前よりも負荷が高くなったと判断した場合は前記サーバ計算機へ転送するデータ要求の数の割合をより低く設定し、

一方、以前よりも負荷が低くなったと判断した場合は前記サーバ計算機へ転送するデータ要求の数の割合をより高く設定することを特徴とするサーバ計算機保護装置を備えた請求項 9 に記載のサーバ計算機。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、クライアントとなる計算機とサーバとなる計算機間のネットワークシステムに関し、特に、意図的にサーバ計算機の処理を妨害する不正なアクセスからサーバとなる計算機を保護するサーバ計算機保護装置に関する。

【0002】

【従来の技術】

近年、インターネット等を利用し、不特定あるいは特定のクライアントとなる

計算機をネットワーク経由でサーバとなる計算機に接続し、クライアントからの要求に応じてサーバからデータを供給することを目的とするクライアント・サーバシステムが広く使われている。

【0003】

インターネット等のネットワークを流れるデータの形式として、宛先情報を付して伝送データを所定の大きさに再構成したパケットが一般に利用されている。パケットは、大まかに分けると、ヘッダとデータ本体とで構成されている。ヘッダには、このパケットの送り元である送信元の計算機を示すIP(Internet Protocol)アドレスと、このパケットの宛先となる計算機のIPアドレスといったアドレス情報をもっている。

【0004】

昨今、このようなネットワークに接続されたシステムに対し、システム的な障害を発生させることを目的としたネットワーク越しの攻撃が増加する傾向にある。たとえば、一つのクライアントから同時に大量のアクセス要求をサーバ計算機に対して行うことにより、攻撃対象となるサーバの稼働を妨げ実質的にサービスを不能にする攻撃方法(以下、DoS攻撃(Denial of Service attack)と表記)がある。

【0005】

この攻撃方法は、システム攻撃を意図しない正当なクライアントからのアクセスとの区別がつきにくいために、サーバ側で攻撃を回避することが極めて困難である。場合によっては複数のクライアントからこの攻撃を受けることもあり、これを特にDDoS攻撃(Distributed Denial of Service attack)と呼んでいる。

【0006】

サーバへの要求がサーバの処理能力を超えるほど大量に送りつけられると、その要求毎に通信処理用の資源、たとえばメモリ領域や回線の帯域などが次々と確保されるためついには不足を来し、妨害を意図していない正当なクライアントからの要求に対しサーバが応答できなくなるか、あるいは大きく滞ってしまうという結果を招く。

【0007】

従来は、これらの攻撃を排除するためにサーバとネットワークの間にサーバ計算機保護装置を配置していた。このサーバ計算機保護装置は、複数回のアクセス要求が繰り返されたもののみを正当なアクセス要求として処理する、または既に正当なアクセスがあったクライアントからのアクセスを正当なアクセス要求として処理し、それ以外のアクセスについてはパケットを破棄するなどの処理を行っていた。

【0008】

しかし、このような方法では、攻撃を意図するクライアントが同じような大量のアクセス要求を行う場合、攻撃を排除できないという問題点があった。

【0009】

一方、上記問題を解決しても、たとえば特定のクライアントが大量のアクセス要求を行うとその通信行為がDoS攻撃であると判断されてしまうため、たとえそれが正当な要求であっても不正なアクセスとみなされる場合があった。DoS攻撃とみなされれば判断されたクライアントの接続は切断されてしまうため、そのクライアントで行っている業務に支障を来す。

【0010】

【特許文献1】 特開2002-16633公報

【0011】

【発明が解決しようとする課題】

本発明は、不特定のクライアントからのDoS攻撃からサーバとなる計算機を保護しながらも、正当なアクセスを行っているクライアントでありながらDoS攻撃を行っている判断された計算機のアクセスも限定的に許容するサーバ計算機保護装置、サーバ計算機保護方法、サーバ計算機保護プログラム及びサーバ計算機を提供することを目的とする。

【0012】

【課題を解決するための手段】

本発明にかかるサーバ計算機保護装置とすれば、
不特定のクライアント計算機によるDoS攻撃からサーバ計算機を保護するサーバ計算機保護装置において、

クライアント計算機から送られてくるデータ要求をサーバ計算機の代わりに受け付けるデータ要求受け付け手段と、

一定期間内に、すべてのクライアント計算機から届いたデータ要求の数を計測するデータ要求数計測手段と、

一定期間内に前記サーバ計算機から前記クライアント計算機へ応答した数を計測するデータ応答数計測手段と、

前記データ応答数計測手段及びデータ要求数計測手段の出力結果を用いて前記サーバ計算機の負荷状態を求めるサーバ負荷算出手段と、

前記サーバ負荷算出手段によって求めた負荷状態に応じて、一定期間内に前記データ要求受け付け手段が受け付けたデータ要求のうちの、該受け付けたデータ要求数に対する一定期間内に前記サーバ計算機へ転送するデータ要求の数の割合を変化させるデータ要求転送手段と、

を備えたことを特徴とするサーバ計算機保護装置
が提供される。

【 0 0 1 3 】

また本発明にかかるサーバ計算機保護方法によれば、
不特定のクライアント計算機によるDoS攻撃からサーバ計算機を保護するサーバ計算機保護方法であって、

クライアント計算機から送られてくるデータ要求をサーバ計算機の代わりに受け付けるステップと、

一定期間内に、すべてのクライアント計算機から届いたデータ要求の数を計測するステップと、

一定期間内に前記サーバ計算機から前記クライアント計算機へ応答した数を計測するステップと、

前記データ要求数及び応答数を用いて前記サーバ計算機の負荷状態を求めるステップと、

前記求めた負荷状態に応じて、一定期間内に受け付けた前記データ要求のうちの、該受け付けたデータ要求数に対する一定期間内に前記サーバ計算機へ転送するデータ要求の数の割合を変化させるデータ要求転送ステップと、

を有することを特徴とするサーバ計算機保護方法
が提供される。

【 0 0 1 4 】

加えて、本発明にかかるサーバ計算機保護プログラムとすれば、
不特定のクライアント計算機によるDoS攻撃からサーバ計算機を保護するサーバ
計算機保護プログラムであって、

所定のクライアント計算機から送られてくるデータ要求をサーバ計算機の代わ
りに受け付けるステップと、

一定期間内に、前記所定のクライアント計算機から届いたデータ要求の数を計
測するステップと、

一定期間内に前記サーバ計算機が前記所定のクライアント計算機へ応答した数
を計測するステップと、

前記データ要求数及び応答数を用いて、前記所定のクライアント計算機に対す
るサーバ計算機の負荷状態を求めるステップと、

前記求めた負荷状態に応じて、一定期間内に受け付けた前記所定のクライアン
ト計算機から送られてくるデータ要求のうちの、該受け付けたデータ要求数に対
する一定期間内に前記サーバ計算機へ転送するデータ要求の数の割合を変化させ
るデータ要求転送ステップと、

を有することを特徴とするサーバ計算機保護プログラム
が提供される。

【 0 0 1 5 】

さらに、本発明にかかるサーバ計算機保護装置を備えたサーバ計算機が提供さ
れる。

【 0 0 1 6 】

【発明の実施の形態】

(第 1 の実施形態)

図 1 に本発明の第 1 の実施形態におけるサーバ計算機保護装置が適用されるネ
ットワーク構成図の一例を示す。図 1 では、ユーザが利用するアプリケーション
が稼動する計算機であるクライアント 1 0 1 - 1、1 0 1 - 2、1 0 1 - 3 と、

ネットワーク 1 0 2 およびサーバ保護装置 1 0 3 が存在する。また、クライアント 1 0 1 で稼動するアプリケーションの実行に伴って必要となるデータの要求を、サーバ計算機保護装置 1 0 3 を介して受信し、さらにサーバ計算機保護装置 1 0 3 を介して送信する計算機であるサーバ 1 0 4 とからなる。クライアント 1 0 1 はサーバ 1 0 4 へ処理に必要なデータを要求し、サーバ 1 0 4 はこの要求に応じてデータを応答するサーバ・クライアント型のネットワークシステムである。クライアント 1 0 1 とサーバ 1 0 4 との通信は、すべてサーバ計算機保護装置 1 0 3 を介して行われる。

【 0 0 1 7 】

図 2 に本発明の第 1 の実施形態におけるサーバ計算機保護装置 1 0 3 の構成図の一例を示す。サーバ計算機保護装置 1 0 3 は、データ要求受け付け部 2 0 1、データ要求転送部 2 0 2、データ要求計測部 2 0 3、データ供給数計測部 2 0 4 および応答確率算出部 2 0 5 からなる。

【 0 0 1 8 】

クライアント 1 0 1 はサーバ計算機保護装置 1 0 3 を介してサーバ 1 0 4 との接続を確立した後、処理に必要なデータをサーバ 1 0 4 に対して要求する。このときデータ要求受け付け部 2 0 1 によって、サーバ 1 0 4 に対する要求を受け付けるとともに、データ要求数計測部 2 0 3 によって受け付け中の要求の数を計測する。

【 0 0 1 9 】

データ要求受け付け部 2 0 1 によって受け付けられた要求は、データ要求転送部 2 0 2 によってサーバ 1 0 4 へと転送される。サーバ 1 0 4 はこの転送された要求に対するデータを、サーバ計算機保護装置 1 0 3 を介して、この要求を行ったクライアント 1 0 1 に向けて送信する。このときサーバ計算機保護装置 1 0 3 が備えるデータ供給数計測部 2 0 4 は、サーバ 1 0 4 のこの送信によって、受け付け済みの要求の完了数を計測する。つまりクライアント 1 0 1 に対してすべての応答が完了したときには、データ要求数計測部 2 0 3 で計測した受け付け中の要求数と、データ供給数計測部 2 0 4 で計測した完了済み要求数が一致することになる。

【 0 0 2 0 】

仮に、データ要求数計測部 2 0 3 で計測された受け付け中の要求数が、データ供給数計測部 2 0 4 で計測した完了済み要求数よりも多い場合を考える。受け付け中の要求数が完了済み要求数よりも多いということはすなわち受け付けた要求に対する処理について、サーバ 1 0 4 の処理が遅れている（処理が重い）ことを意味する。完了済み要求数よりも受け付け中の要求数が増加していけば行くほどサーバ 1 0 4 の応答は遅延し、ひいてはサーバ 1 0 4 が提供しているサービスがすべて停止してしまうことも考えられる。この状態はサーバ 1 0 4 がクライアント 1 0 1 から DoS 攻撃を受けた状態と同じである。サーバ 1 0 4 の管理者はサーバ 1 0 4 の停止を回避するため、クライアント 1 0 1 からサーバ 1 0 4 へ送信される要求を速やかに停止させなければならない。

【 0 0 2 1 】

しかしながらクライアント 1 0 1 はあくまで正当なデータ要求を行っているだけであるとすれば、この決定によってクライアント 1 0 1 で稼動するアプリケーションの処理が中断あるいは処理そのものがないことになる。

【 0 0 2 2 】

上記したような不具合を緩和するために、応答確率算出部 2 0 5 は受け付け中の要求数と完了済み要求数の差を元に、応答確率を少なくとも指示を行う都度算出し、これをデータ要求転送部 2 0 2 に指示する。ここでいう応答確率とは、一定期間内に受け付けたクライアント 1 0 1 からのデータ要求の数に対して、サーバ 1 0 4 が一定期間内に応答したデータ応答数の比率をいう。データ要求転送部 2 0 2 は、この値が大きければ一定期間内に受け付けたデータ要求のうち一定期間内にサーバ 1 0 4 へ転送するデータ要求の数を増やし、逆に小さければ一定期間内にサーバ 1 0 4 へ転送するデータ要求の数を減らす。

【 0 0 2 3 】

一定期間内に転送される要求数を減らしたために、データ要求転送部 2 0 2 によって転送されなかったデータ要求は、データ要求受け付け部 2 0 1 から破棄される。あるいは破棄することなくデータ要求受け付け部 2 0 1 に保留するようにしてもよい。ただし破棄をせずデータ要求を保留する場合には、保留したデータ

要求を、新たなデータ要求とは非同期に転送するための構成を必要とするが、本実施形態では説明しない。

【 0 0 2 4 】

応答確率算出部 2 0 5 は、受け付け中の要求数と完了済み要求数との差が少なくなるとサーバ 1 0 4 の負荷が軽いと判断して応答確率を高く算出し、また各要求数の差が大きくなるとサーバ 1 0 4 の負荷が高いと判断し応答確率を低く算出する。

【 0 0 2 5 】

上記のように構成すると、サーバに負荷をかけて停止させるようなDoS攻撃の影響を緩和させるとともに、正当なデータ要求を行っているにもかかわらずDoS攻撃をしていると判定されたクライアントの処理も停止させることのないサーバ計算機保護装置とすることができる。

【 0 0 2 6 】

なお、データ要求数計測部 2 0 3 の受け付け中の要求数とデータ供給数計測部 2 0 4 が計測する完了済み要求数のそれぞれの数は、たとえば前者を加算、後者を減算するようにして差分値のみを保持するようにしてもよい。結果的に両者の比較が可能な手段で蓄積されていれば足りる。

【 0 0 2 7 】

図 3 に本発明の第 1 の実施形態におけるサーバ計算機保護装置の動作フローの一例を示す。

【 0 0 2 8 】

サーバ計算機保護装置 1 0 3 を介してクライアント 1 0 1 からサーバ 1 0 4 への接続が確立された後、クライアント 1 0 1 からサーバ 1 0 4 に向けてデータ要求がされるのを待つ (S 1)。データの要求がされたならばデータ要求数計測部 2 0 3 によって、応答確率算出部 2 0 5 が保持する受け付け中の要求数を 1 増加させる (S 2)。

【 0 0 2 9 】

データ要求受け付け部 2 0 1 によって受け付けられたクライアント 1 0 1 からのデータ要求は、データ要求転送部 2 0 2 によってサーバ 1 0 4 へ転送しても良

いものかどうか判断される（S3）。ステップS3の判断に際しては、未完了の受け付け中の要求数が使用される。

【0030】

一定期間内のデータ応答数が一定期間内に受け付けたデータ要求数に近いほど、つまり未完了の受け付け要求数が少ないほどサーバ104の負荷が軽いと判断できる。逆に、一定期間内に受け付けたデータ要求数よりも一定期間内のデータ応答数が少ないほど、つまり未完了の受け付け要求数が多いほどサーバ104がデータ要求に対する処理を所定の時間内に完了できていない、すなわち負荷が重いと判断できる。このときの負荷が極めて重い場合には、サーバ104はDoS攻撃を受けている可能性が高いと判断できる。

【0031】

上記したような理由からステップS3の判定に、未完了の受け付け要求数を、サーバ104の負荷状態として採用することができる。これはすなわち未完了の受け付け要求数が、サーバ104がDoS攻撃を受けていかどうかという判別にも使用できることを意味している。ステップS3では、この未完了の受け付け要求数に応じてクライアント101からの新たなデータ要求を転送しても良いかどうかを判断する。未完了の受け付け要求数がより少なければサーバ104に余裕があるので新たなデータ要求を転送すべきと判断し、逆により多ければDoS攻撃を受けている可能性があるので新たなデータ要求を破棄すべきと判断する。

【0032】

このときサーバ104にクライアント101からの新たなデータ要求を転送すべきと判断したときは、このデータ要求をサーバ104に転送する（S4）。一方、転送しないと判断したときはこのデータ要求をデータ要求受け付け部201から破棄し、再びクライアント101からの新たなデータ要求を待つ（S1）。

【0033】

クライアント101からのデータ要求をサーバ104に転送したときには、次にこのデータ要求に対するサーバ104からの応答があるので、これをクライアント101に対して転送する（S5）。

【0034】

そしてこの応答からデータ供給数計測部 2 0 4 によって完了済みの要求を計測し、応答確率算出部 2 0 5 が保持する受け付け中の要求数を 1 減少させる (S 6) 。 クライアント 1 0 1 からサーバ 1 0 4 への接続が確立されたままならば再び同様の動作フローを繰り返し、クライアント 1 0 1 からサーバ 1 0 4 に向けて新たなデータ要求がされるのを待つ (S 1) 。

【 0 0 3 5 】

このようなフローによるサーバ計算機保護方法によれば、サーバに負荷をかけて停止させるようなDoS攻撃の影響を緩和させるとともに、正当なデータ要求を行っているにもかかわらずDoS攻撃をしていると判定されたクライアントの処理も停止させることのないサーバ計算機保護装置とすることができる。

【 0 0 3 6 】

(第 2 の実施形態)

図 1 に本発明の第 2 の実施形態における、サーバ計算機保護装置が適用されるネットワーク構成図の一例を示す。図 1 では、ユーザが利用するアプリケーションが稼動する計算機であるクライアント 1 0 1 - 1、1 0 1 - 2、1 0 1 - 3 と、ネットワーク 1 0 2 およびサーバ保護装置 1 0 3 が存在する。また、クライアント 1 0 1 で稼動するアプリケーションの実行に伴って必要となるデータの要求を、サーバ計算機保護装置 1 0 3 を介して受信し、さらにサーバ計算機保護装置 1 0 3 を介して送信する計算機であるサーバ 1 0 4 とからなる。クライアント 1 0 1 はサーバ 1 0 4 へ処理に必要なデータを要求し、サーバ 1 0 4 はこの要求に応じてデータを応答するサーバ・クライアント型のネットワークシステムである。クライアント 1 0 1 とサーバ 1 0 4 との通信は、すべてサーバ計算機保護装置 1 0 3 を介して行われる。

【 0 0 3 7 】

図 4 に本発明の第 2 の実施形態におけるサーバ計算機保護装置 1 0 3 の構成図の一例を示す。サーバ計算機保護装置 1 0 3 は、データ要求受け付け部 2 0 1、データ要求転送部 2 0 2、データ要求計測部 2 0 3、データ供給数計測部 2 0 4 および応答確率算出部 2 0 5 からなる。図 2 に示した本発明の第 1 の実施形態におけるサーバ計算機保護装置 1 0 3 との相違は、データ要求数計測部 2 0 3 及び

応答確率算出部 2 0 5 を複数備えていることである。これら複数の各計測部は、複数あるクライアント 1 0 1（たとえばクライアント 1 0 1 - 1、1 0 1 - 2、1 0 1 - 3）のそれぞれから送信されるデータ要求の転送を、それぞれのクライアントごとに処理するために構成されている。クライアントごとの処理を行うためには、処理すべき要求がどのクライアントが発信したものであるかの判別が必要となる。この判別は、各クライアントから送信されるデータ要求に含まれるパケットのヘッダ情報の送信元を示す I P アドレスを参照することにより可能である。同様にサーバが行うサーバ応答の宛先のクライアントも、サーバ応答に含まれるパケットのヘッダ情報の宛先を示す I P アドレスを参照することにより判別可能である。

【 0 0 3 8 】

各構成要素の動作は第 1 の実施形態のものと同一である。

【 0 0 3 9 】

図 5 に本発明の第 2 の実施形態におけるサーバ計算機保護装置の動作フローの一例を示す。

【 0 0 4 0 】

サーバ計算機保護装置 1 0 3 を介してクライアント 1 0 1 からサーバ 1 0 4 への接続が確立され、そのクライアント 1 0 1 にデータ要求数計測部 2 0 3 と応答確率算出部 2 0 5 の組が割り当てられた後、クライアント 1 0 1 からサーバ 1 0 4 に向けてデータ要求がされるのを待つ（S 1）。データの要求がされたならばそのデータ要求を行ったクライアント 1 0 1 に割り当てられているデータ要求数計測部 2 0 3 によって、その組となっている応答確率算出部 2 0 5 が保持する受け付け中の要求数を 1 増加させる（S 7）。

【 0 0 4 1 】

データ要求受け付け部 2 0 1 によって受け付けられた所定のクライアント 1 0 1 からのデータ要求は、データ要求転送部 2 0 2 によってサーバ 1 0 4 へ転送しても良いものかどうか判断される（S 3）。ステップ S 3 の判断に際しては、未完了の受け付け中の要求数が使用される。

【 0 0 4 2 】

一定期間内のデータ応答数が一定期間内に受け付けたデータ要求数に近いほど、つまり未完了の受け付け要求数が少ないほど所定のクライアント 1 0 1 によるサーバ 1 0 4 の負荷が軽いと判断できる。逆に、一定期間内に受け付けたデータ要求数よりも一定期間内のデータ応答数が少ないほど、つまり未完了の受け付け要求数が多いほどサーバ 1 0 4 が所定のクライアント 1 0 1 によるデータ要求に対する処理を所定の時間内に完了できていない、すなわち負荷が重いと判断できる。このときの負荷が極めて重い場合には、サーバ 1 0 4 はDoS攻撃を受けている可能性が高いと判断できる。

【 0 0 4 3 】

上記したような理由からステップ S 3 の判定に、未完了の受け付け要求数を、サーバ 1 0 4 の負荷状態として採用することができる。これはすなわち未完了の受け付け要求数が、サーバ 1 0 4 がDoS攻撃を受けていかどうかという判別にも使用できることを意味している。ステップ S 3 では、この未完了の受け付け要求数に応じて所定のクライアント 1 0 1 からの新たなデータ要求を転送しても良いかどうかを判断する。未完了の受け付け要求数がより少なければサーバ 1 0 4 に余裕があるので新たなデータ要求を転送すべきと判断し、逆により多ければDoS攻撃を受けている可能性があるので新たなデータ要求を破棄すべきと判断する。

【 0 0 4 4 】

このときサーバ 1 0 4 に所定のクライアント 1 0 1 からの新たなデータ要求を転送すべきと判断したときは、このデータ要求をサーバ 1 0 4 に転送する（S 8）。一方、転送しないと判断したときはこのデータ要求をデータ要求受け付け部 2 0 1 から破棄し、再び所定のクライアント 1 0 1 からの新たなデータ要求を待つ（S 1）。

【 0 0 4 5 】

所定のクライアント 1 0 1 からのデータ要求をサーバ 1 0 4 に転送したときには、次にこのデータ要求に対するサーバ 1 0 4 からの応答があるので、これを所定のクライアント 1 0 1 に対して転送する（S 5）。

【 0 0 4 6 】

そしてこの応答からデータ供給数計測部 2 0 4 によって完了済みの要求を計測

し、所定のクライアント 1 0 1 に割り当てられた応答確率算出部 2 0 5 が保持する受け付け中の要求数を 1 減少させる (S 9)。 所定のクライアント 1 0 1 からサーバ 1 0 4 への接続が確立されたままならば再び同様の動作フローを繰り返す、所定のクライアント 1 0 1 からサーバ 1 0 4 に向けて新たなデータ要求がされるのを待つ (S 1)。

【 0 0 4 7 】

このようなフローによるサーバ計算機保護方法によれば、サーバに負荷をかけて停止させるようなDoS攻撃の影響を緩和させるとともに、正当なデータ要求を行っているにもかかわらずDoS攻撃をしていると判定されたクライアントを停止させることなく、またクライアントごとのきめ細かなサーバ計算機保護のための制御を可能としたサーバ計算機保護装置とすることができる。

【 0 0 4 8 】

(第 2 の実施形態における変形例)

本実施形態の変形例として、サーバ 1 0 4 に本実施形態にかかるサーバ計算機保護装置 1 0 3 の構成を組み合わせたサーバ 1 0 4 とすることができる。このように構成するとクライアント 1 0 1 からのデータ要求を処理するサーバ 1 0 4 と、このサーバ 1 0 4 を不特定のクライアント 1 0 1 からのDoS攻撃から保護する目的で設けるサーバ計算機保護装置 1 0 3 とを分離して個別に構成する必要がない。よってサーバ計算機保護装置 1 0 3 とサーバ 1 0 4 との通信をネットワーク等を介して行う必要がなくなり、通信に要していた時間を排除することができる。また複数の筐体により構成したサーバ計算機保護装置 1 0 3 によって保護されたサーバ 1 0 4 の場合と比較して、同様の機能を 1 つの筐体で提供できる可能性があり、この場合には設置に必要なスペースを削減することができる。

【 0 0 4 9 】

【発明の効果】

不特定のクライアントからのDoS攻撃からサーバとなる計算機を保護しながらも、正当なアクセスを行っているクライアントでありながらDoS攻撃を行っている判断された計算機のアクセスも限定的に許容するサーバ計算機保護装置とすることができる。

【図面の簡単な説明】

【図 1】 本発明の第 1 の実施形態にかかるサーバ計算機保護装置が適用されるネットワーク構成図の一例を示す図である。

【図 2】 本発明の第 1 の実施形態にかかるサーバ計算機保護装置の構成図の一例を示す図である。

【図 3】 本発明の第 1 の実施形態にかかるサーバ計算機保護装置の動作フローの一例を示す図である。

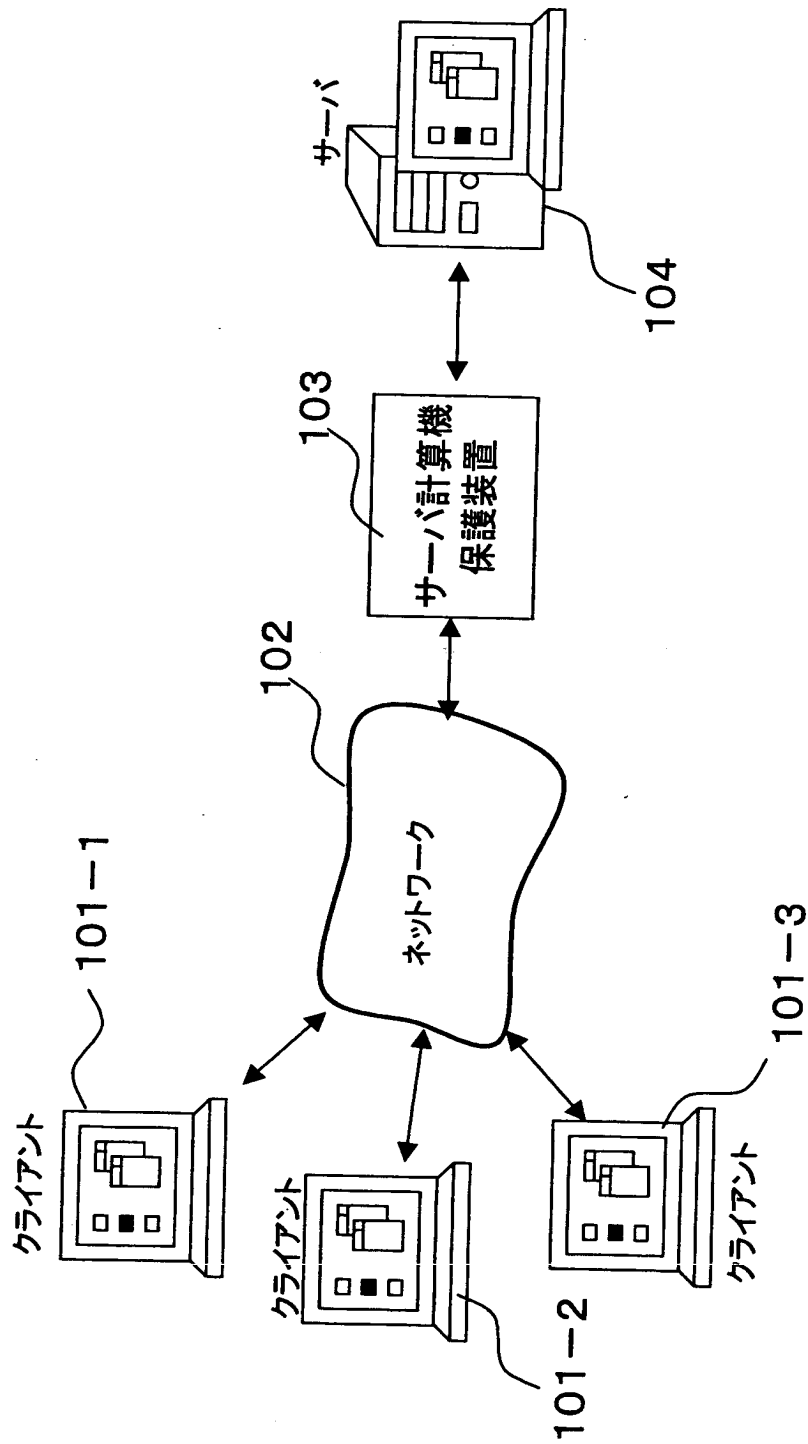
【図 4】 本発明の第 2 の実施形態にかかるサーバ計算機保護装置の構成図の一例を示す図である。

【図 5】 本発明の第 2 の実施形態にかかるサーバ計算機保護装置の動作フローの一例を示す図である。

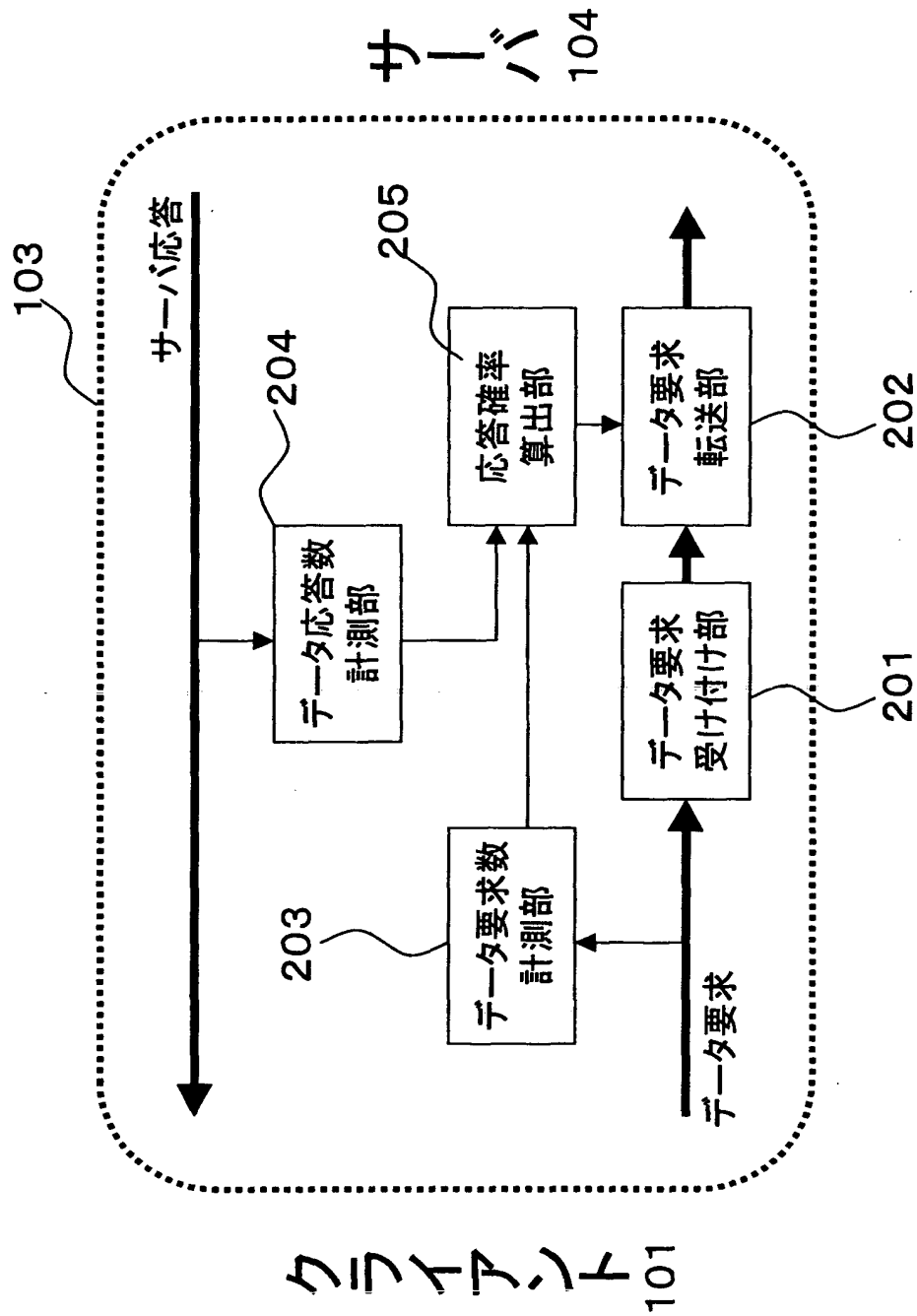
【符号の説明】

1 0 1 - 1	．．．	クライアント
1 0 1 - 2	．．．	クライアント
1 0 1 - 3	．．．	クライアント
1 0 2	．．．	ネットワーク
1 0 3	．．．	サーバ計算機保護装置
1 0 4	．．．	サーバ
2 0 1	．．．	データ要求受け付け部
2 0 2	．．．	データ要求転送部
2 0 3	．．．	データ要求数計測部
2 0 4	．．．	データ供給数計測部
2 0 5	．．．	応答確率算出部

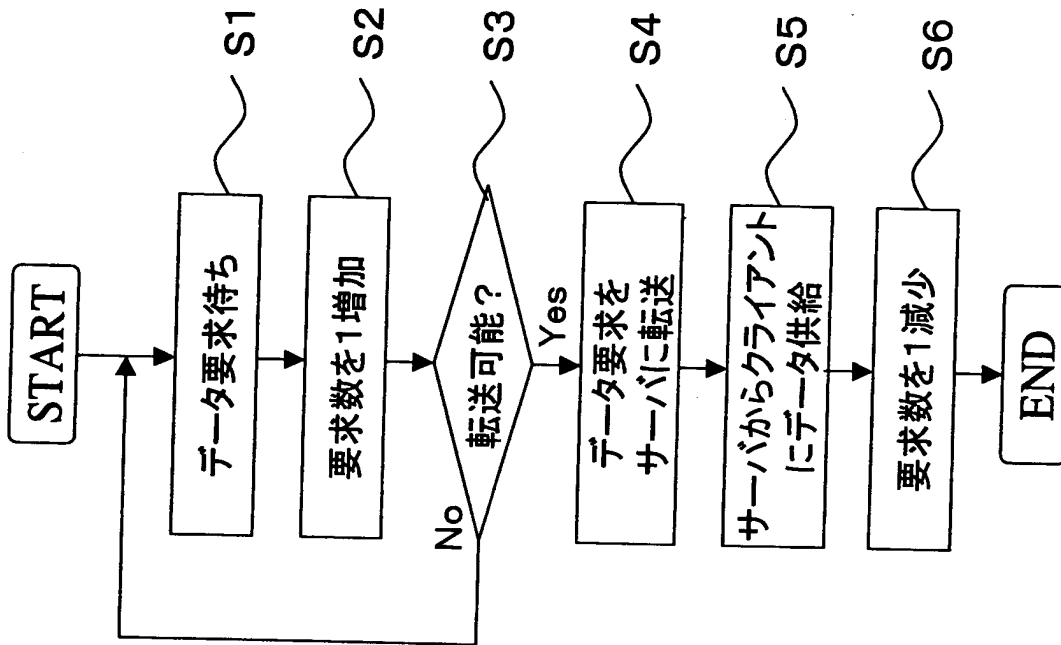
【書類名】 図面
【図1】



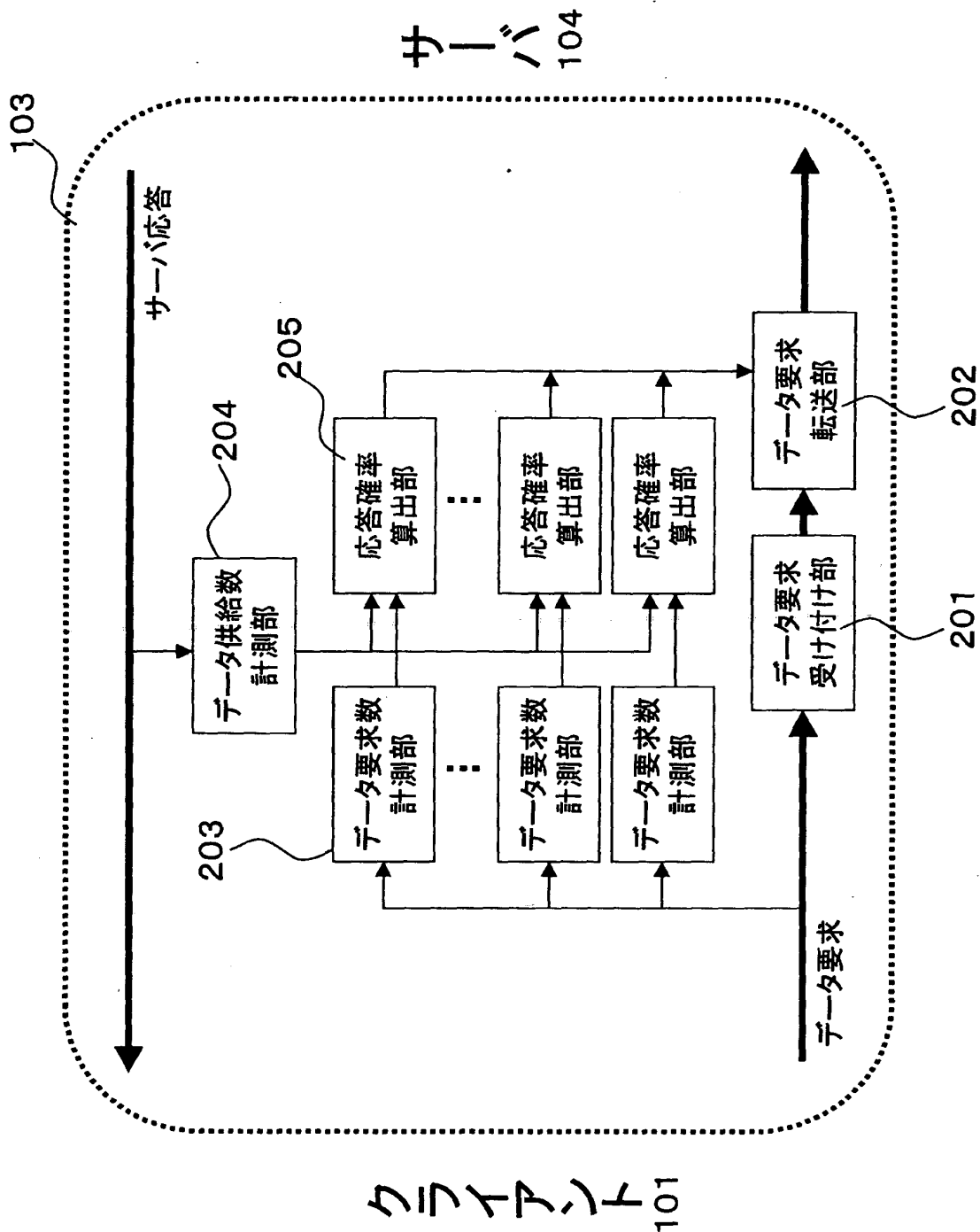
【図 2】



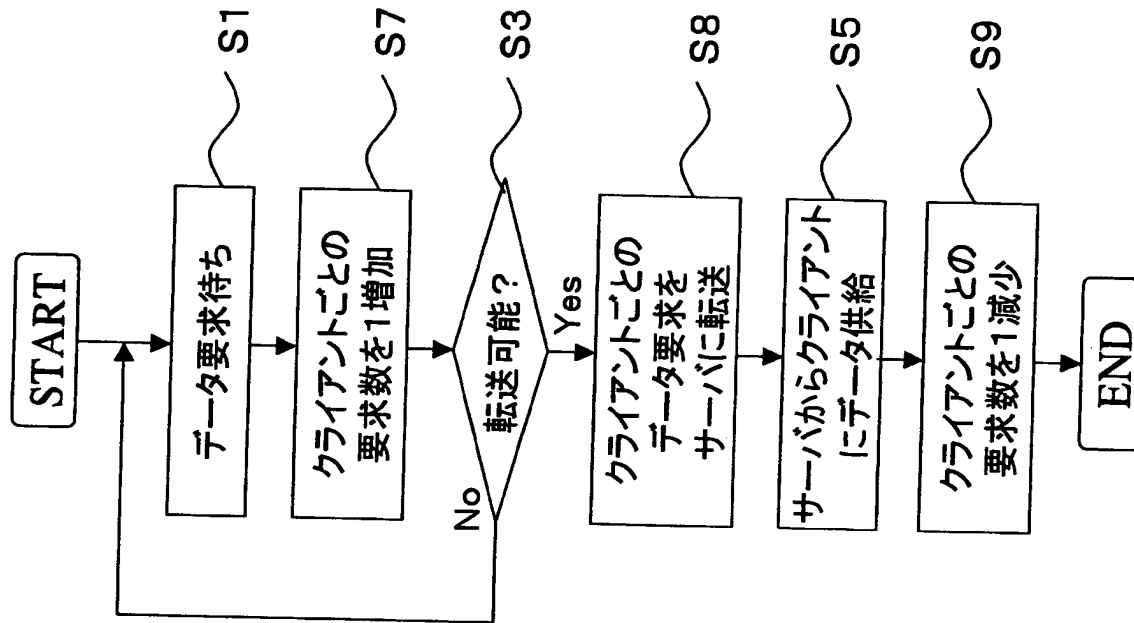
【図3】



【図4】



【図 5】



【書類名】 要約書

【要約】

【課題】 不特定のクライアントからのDoS攻撃からサーバとなる計算機を保護しながら、正当なアクセスを行っているクライアントでありながらDoS攻撃を行っていると判断された計算機のアクセスも限定的に許容するサーバ計算機保護装置を提供することを目的とする。

【解決手段】 サーバとなる計算機に対してデータ要求される数と、これに応答するサーバのデータ応答の数を用いてサーバ計算機の負荷状態を求め、この負荷状態に応じてサーバに転送するデータ要求の割合を変化させる手段を備えたサーバ計算機保護装置とする。

【選択図】 図2

認定・付加情報

特許出願の番号	特願2002-280289	
受付番号	50201438074	
書類名	特許願	
担当官	第八担当上席	0097
作成日	平成14年 9月27日	

<認定情報・付加情報>

【提出日】	平成14年 9月26日
-------	-------------

出 願 人 履 歴 情 報

識別番号 [000003078]

1. 変更年月日	2001年 7月 2日
[変更理由]	住所変更
住 所	東京都港区芝浦一丁目1番1号
氏 名	株式会社東芝